PTO/SB/08B (04-03)
Approved for use through 04/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Compl t if Kn wn die for form 1449/PTO Applicati n Number 10/000,396 INFORMATION DISCLOSURE Filing Dat November 30, 2001 STATEMENT BY APPLICANT **First Named Inventor** John A. Copeland III Art Unit 2131 <u>JUN 2 6 20</u>03 (Use as many sheets as necessary) **Examiner Name** Technology Center 2100

Attorney Docket Number

10775-36246

Sheet

2

		NON PATENT LITERATURE DOCUMENTS	
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T²
	? 	KATO, et. al. "A Real-Time Intrusion Detection System for Large Scale Networks and its Evaluations" leice Transactions on Communications, Institute of Electronices Information and Comm. Eng. Tokyo, Japan: November 1999, pages 1817-1825.	
RB		DEBAR, et. al. "Towards a Taxonomy of Intrusion-Detection Systems" Computer Networks, Elsevier Science Publishers, B.V., Amsterdam, NL 23 April 1999, pages 805-822	
		·	
		1 00	

Examiner Date Signature Considered

*EXAMINER: Initial if reference considered, whether or not citation is in contconsidered. Include copy of this form with pext communication to applicant. helher of not cliation is in conformance with MPEP 609. Draw line through citation if not in conformance and not

Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The Information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35/U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

PTO/SB/08A (04-03)
Approved for use through 04/30/2003, OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE experience Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

e for form 1449/PTO

JUN. 2 4 2003

Sheet 2

Examiner

Signature

Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Compl t if Known				
Application Number	10/000,396			
Filing Date	November 30, 2001			
First Named Inventor	John A. Copeland III			
Art Unit	2131			
Examiner Name				
Attorney Docket Number	10775 36346			

U. S. PATENT DOCUMENTS Examiner **Document Number Publication Date** Name of Patentee or Pages, Columns, Lines, Where MM-DD-YYYY **Applicant of Cited Document** Initials* No Relevant Passages or Relevant Number-Kind Code^{2 (# known)} Figures Appear US: US-บรus-US-JUN 2 6 2003 US-US-Technology Center 2100 US-US-US-US-US-US-US-US-US-ÜS-US-

Examiner Initials*	Cite No.	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages	
10		Country Code ³ "Number ⁴ "Kind Code ⁵ (if known)	MM-DD-YYYY		Or Relevant Figures Appear	٦٠ ا
112		PCT/US00/29490	05-03-2001	Diep, et. al.		
DA		PCT/US99/29080	06-15-2000	Diep, Thanh A.		
MO						
					•	L
				ļ,, <u>.</u>		

*EXAMINER: Initial Metitience considered, whether of not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.bspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. Applicant is to place a check mark here if English language

Date Considered

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

THE PRADEMARY

PTO/SB/08A (10-01)

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

of Sheet

		7		
C mplete if Known				
Application Number	10/000,396			
Filing Date	11/30/2001			
First Named Inventor	John A. Copeland III			
Art Unit	2131			
Examiner Name				
Attomey Docket Number	10775-36246	_		

		•	U.S. PATE	NT DOCUMENTS	
Examiner Initials		Qocument Number Number- Kind Code ² (if known	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
1210		US6,182,226B1	01-30-2001	Reid, et. al.	
j	i	us- 5.991.881	11-23-1999	Conklin, et. al.	
NA	<u></u>	us- 5,970,227	10-19-1999	Dayan, et. al.	
100		US-			
		US-			
		US-			
	<u> </u>	US-			
		US-			
		US-			
		US-			
	l	US-			RECEIVED
		US-			
	<u> </u>	us-		an annual an	MAY 2-1 2003
		us.			
	<u>]</u>	∪S·			Technology Center 210
	ļ	.us- ,			leculology center 2.
	.	us-	· · · · · · · · · · · · · · · · · · ·		
	<u>.</u>	US-		المناسب المارية والمستقلينية والمراج والمراج والمراج	
		us-		and the second s	
		US-		<u> </u>	

	FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No. ¹	Foreign Patent Document Country Code 3 - Number 4 - Kind Code 3 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Т6	
i							
	<u> </u>			<u> </u>		<u> </u>	

Date Examiner Signature Considered

*EXAMINER: Initial I reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.usplo.gov or MPEP 901.04. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. 8 Applicant is to place a check mark here if English language Translation is attached. English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

PTO/SB/08B (10-01)

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

der the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB

+

Substitute for form 1449B/PTO

Sheet

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

of

Filing Date 11/30/2001
First Named Inventor John A. Copeland. III
Group Art Unit 2131
Examiner Name
Attorney Docket Number 10/775-36246

Complet if Known

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the Examine item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue COPELAND, JOHN A., et. al., "IP Flow Identification for IP Traffic Carried Over Switched Networks." The International Journal of Computer and Telecommunications Networking COMPUTER NETWORKS 31 (1999), pp. 493-504. COOPER, MARK "An Overview of Intrusion Detection Systems," Zinetica White Paper, (www.xinetica.com) November 19, 2001. NEWMAN, P., et. al. "RFC 1953: Ipsilon Flow Management Protocol Specification for IPv4 Version 1.0" (www.xyweb.com/rfc/rfc1953.html) May 19, 1999. PAXSON, VERN, "Bro: A System for Detecting Network Intruders in Real-Time," 7th USENIX Security Symposium, Lawrence Berkkeley National Laboratory, San Antonio, TX January 26-29, MUKHERJEE, BISWANATH, et. al., "Network Intrusion Detection," IEEE Network, May/June 1994. 'Network-vs Host-Based Intrusion Detection: A Guide to Intrusion Detection," ISS Internet Security Systems, October 2, 1998, Atlanta, GA. BARFORD, PAUL, ct. al. "Characteristics of Network Traffic Flow Anomalies," ACM SIGCOMM Internet Measurement Workshop 2001 (http://www.cs.wisc.edu/pb/ublications.html) July 2001. FRINCKE, DEBORAH, et. al., "A Framework for Cooperative Intrusion Detection" 21st National Information Systems Security Conference, Oct. 1998, Crystal City, VA. Phrack Magazine, Volume 8, Issue 53, July 8, 1998, Article 11 of 15. "LANSleuth Fact Sheet," LANSleuth LAN Analyzer for Ethernet and Token Ring Networks, (www.lansleuth.com/features.html), Aurora, Illinois. RECEIVED "LANSleuth General Features," (www.lansleuth.com/features.html), Aurora, Illinois. MAY 2 2003 Technology Center 2100

Examiner Signature Date Considered 5/6/12/6

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional).

Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → +	Please type a	plus sign	(+) inside	this box	→	T+
---	---------------	-----------	------------	----------	---	----

of

Sheet

10775-36246

PTO/SB/08A (10-96)
Approved for use through 10/31/99. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number. Complet if Kn wn Substitute for form 1449A/PTO **Application Number** 10/000,396 INFORMATION DISCLOSURE 11/30/2001 Filing Date STATEMENT BY APPLICANT John A. Copeland, III **First Named Inventor** Group Art Unit (use as many sheets as necessary) **Examiner Name**

Attorney Docket Number

				U.S. PATENT DOCI	UMENTS	
Examiner nitials\	Cite No.1	U.S. Patent Number	Kind Code ²	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant
ANNI MARIE		6 553 34	(If known)	Smaha, et al.	09-17-1996	Figures Appear
7	$\overline{}$	5,557,74 5,621,88		Lermuzeaux, et al.	04-15-1997	RECE
A no		6,275,942		Bernhard, et al.	08-14-2001	
		6,321,338		Porras, et al.	11-20-2001	Aug
μ	\neg	-,-,,				104 1 9 2000
						Technology
						Technology Center
Ì						
				·		
			-			
		- ,				
					 	
	<u></u>			· · · · · · · · · · · · · · · · · · ·		

				FORE	IGN PATENT DOCUMENT	rs		
Examiner	Cite	Foreign Patent Document		Name of Patentee or	Date of Publication of	Pages, Columns, Lines, Where Relevant	Ţ	
Initials*	No.1	Office ³	Number ⁴	Kind Code ⁵ (if known)	Applicant of Cited Document	Cited Document MM-DD-YYYY	Passages or Relevant	T8
								L^-
	•	·						
					•			\top
								T
								\Box
,								
								Γ
	<u></u>							
			I.	•	4			
			K/	,	//			

Date Examiner Considered Signature

*EXAMINER: Initial if presence considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

¹ Unique citation designation number. 2 See attached Kinds of U.S./Patent Documents. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 4 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box → +	٦
---	---

PTO/SB/08B (10-96)
Approved for use through 10/31/99. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

	(use as man)	3110013	49 1166633	ary
Shoot		of		

Complete if Known				
Application Number	10/000,396			
Filing Date	11/30/2001			
First Named Inventor	John A. Copeland, III			
Group Art Unit				
Examiner Name				
Attorney Docket Number	10775-36246			

Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue publisher, city and/or country where published. Copeland, John A., et al, "IP Flow Identification for IP Traffic Carried Over Switched International Journal of Computer and Telecommmunications Networking COMPUT (1999), pp. 493-504 Cooper, Mark "An Overview of Instrusion Detection Systems," Xinetica White Paper, (www.xinetica.com) November 19, 2001 Newman, P., et al. "RFC 1953: Ipsilon Flow Management Protocol Specification for (www.xyweb.com/rfc/rfc1953.html) May 19, 1999	number(s), d Networks," The ER NETWORKS 31	T²
International Journal of Computer and Telecommmunications Networking COMPUT (1999), pp. 493-504 Cooper, Mark "An Overview of Instrusion Detection Systems," Xinetica White Paper, (www.xinetica.com) November 19, 2001 Newman, P., et al. "RFC 1953: Ipsilon Flow Management Protocol Specification for (www.xinetica.com) (Sec. 1963 http://doi.org/10.1000)	ER NETWORKS 31 IPv4 Version 1.0"	
(www.xinetica.com) November 19, 2001 Newman, P., et al. "RFC 1953: Ipsilon Flow Management Protocol Specification for (www.xinetica.com) November 19, 2001	IPv4 Version 1.0"	
11 /		
	MECE	11 7 1
	1110 -	/V#
	HUL I O	200
	Technology Cen	iter 2
		+
		\prod
	 .	$\perp \perp$
		Ħ
	×	$\perp \perp$
xaminer Dat a	= 1 - 1 - 1	\equiv

*EXAMINER: Initial if reference considered, when er or not citation/is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Considered

Burden Hour Stalement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner-for Patents, Washington, DC 20231.

Signature

¹ Unique citation designation number. ² Applicant is to place a €heck mark here if English language Translation is attached.